

# Cybersecurity Analyst Possible Interview Questions

Q: What is Pentest

A: "Pentest" is short for "penetration test", and involves having a trusted security expert attack a system for discovering, and repairing, security vulnerabilities before malicious attackers can exploit them.

Q: What is Social engineering

A: Social engineering" refers to the use of humans as an attack vector to compromise a system. It involves fooling or otherwise manipulating human personnel into revealing information or performing actions on the attacker's behalf. Phishing is Common social engineering techniques

Q: What is man-in-the-middle attack

A: A man-in-the-middle attack is one in which the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping

**Q: Explain what is phishing? How it can be prevented?**

A: Phishing is a technique that deceit people to obtain data from users. The social engineer tries to impersonate genuine website webpage like yahoo or face-book and will ask the user to enter their password and account ID.

It can be prevented by

- Having a guard against spam
- Communicating personal information through secure websites only
- Download files or attachments in emails from unknown senders
- Never e-mail financial information
- Beware of links in e-mails that ask for personal information
- Ignore entering personal information in a pop-up screen

**Q : Mention what are web server vulnerabilities?**

A: The common weakness or vulnerabilities that the web server can take an advantage of are

- Default settings
  - Misconfiguration
  - Bugs in operating system and web servers
-

Q: WHAT'S THE DIFFERENCE BETWEEN ENCODING, ENCRYPTION, AND HASHING?

**Answer**

- Encoding is designed to protect the integrity of data as it crosses networks and systems, i.e. to keep its original message upon arriving, and it isn't primarily a security function. It is easily reversible.
  - Encryption is designed purely for confidentiality and is reversible only if you have the appropriate key/keys.
  - Hashing the operation is one-way (non-reversible), and the output is of a fixed length that is usually much smaller than the input.
- 

Q: WHAT'S MORE SECURE, SSL OR HTTPS?

Answer: Trick question: ????? Hahaha.

---

WHAT IS CROSS-SITE REQUEST FORGERY? Desired answer: when an attacker gets a victim's browser to make requests, ideally with their credentials included, without their knowing. A solid example of this is when an IMG tag points to a URL associated with an action, e.g. <http://foo.com/logout/>. A victim just loading that page could potentially get logged out from foo.com, and their browser would have made the action, not them (since browsers load all IMG tags automatically).

WHAT EXACTLY IS CROSS SITE SCRIPTING? We're looking for them to say anything regarding an attacker getting a victim to run script content (usually JavaScript) within their browser.

---

Q: WHAT ARE THE COMMON DEFENSES AGAINST XSS? Input Validation/Output Sanitization, with focus on the latter.

Q: WHAT'S THE DIFFERENCE BETWEEN A THREAT, VULNERABILITY, AND A RISK?

## Technical Questions Relating to IT Security:

### 1. Introduce /tell us about yourself:

I am an IT Security Analyst with over **X** years of experience in X, X and X (**mention a few of IT Security projects/Tasks on your resume and/or previous work relevant to the job**). I have Bachelors of Science (BS) in **X**. I am currently a Senior IT Security Analyst with **X**, which is an IT security or consulting company. Prior to this, I worked as an IT Security Analyst with **X**., which is also an IT consulting firm located in **X** Maryland. (**i.e., customize and say things in your own words as necessary but keep it short and to your years of experience, last two employers and education**)

### 2. What did you do as an IT Security Analyst? Or what is your typical day like? What do you do on daily basis, or what is your role in your IT Security team?

- a. As an IT Security analyst, I perform the role of an Assessor and perform security control assessment (SCA) as part of Certification and Accreditation (C&A) and continuous monitoring testing/projects, I also perform a review of security documents updated by ISSO to confirm they are FISMA compliant, review and certifying/validation of items uploaded into POA&M tracking tool in support of remediated/closed findings. (**Silent Note: You can also mention two or more of the following tasks**): vulnerability scanning, vulnerability assessment (i.e., ability to analyze, interpret and use/include vulnerability scanning result in the C&A package SAR report), penetration testing, development and updating of IT Security policies and procedures, Assessment & Authorization (A&A) package development and review (**such as FIPS 199 categorization, E-Authentication risk assessment, System Security Plan (SSP), privacy threshold analysis (PTA), Privacy Impact Assessment (PIA), POA&M and Contingency Plan, for completeness and compliance with NIST guidance**), audit support/coordination, incident response(or management which involves correction of identified security incidents) and PCI DSS compliance audit. NIST, ISO, Sans-20 Critical Security Controls standards or PCI Data Security Standards are used to determine if security controls are effective and we prepare report on IT weaknesses and recommendation for noted exceptions. (**Silent Note: Also remember you could be engaged through your firm/company, or you could be an independent contractor working for yourself or your own registered company to assist clients with these projects/tasks**) See the ISSO's typical functions in item 2c below.

Or

- b. IT Security Analyst Role alternative longer Responses that highlight your different projects and the reasons behind them when assigned to a particular department X or federal agency (remember to say things in your own words):

- (i) I assist with FISMA compliance and the preparation of systems Certification and Accreditation (C&A) packages required for systems before they are moved into operation, when major changes occur in them or every 3 years.
- (ii) My day starts with checking on my assigned systems, and I have **X** (ranging from 7-10 systems) of them, to **make sure**:

- they continue to be FISMA compliant. This involves making sure that their C&A Packages remain current and have been reviewed in the last one year (these are SP, CP, CPT (CP test result) and documented security procedures).
  - I also make sure that the security assessment report (SAR) and the authority to operate (ATO) are within their 3-year life-span, and
  - that the systems' POA&Ms have been closed or update provided where necessary in the POA&M tracking tool named CSAM to ensure no system weakness remediation milestone is in delayed status since these are the normal causes of FISMA failing grades. **(Silent note, except asked:** if impossible to close or resolve the POA&Ms before the scheduled completion date, the completion date may be changed/moved forward if within the initial 6 months of the finding, else an extension may be requested with a waiver for another 6 months)
  - I reach out to the systems security officers (ISSOs) and work with them to make sure things are in order with those systems.
  - I provide weekly status report to the client on these systems and any C&A package update that is taking place on them.
- (iii) Next, I'm reviewing the C&A packages that have expired on my systems which have been updated by the ISSOs. As indicated earlier, they need to keep them current with annual updates to the documents. These documents are reviewed by me after every update to ensure the updates are compliant with NIST 800-53 standards and enterprise policies.
- (iv) Sometimes, there may be security control assessment (SCA) going on some of these systems that I need to conduct interview on with their system owners. This involves performing a walkthrough of the controls selected from NIST-800-53 for these systems based on their FIPS 199 security categorization, and getting information from the system owners or their ISSOs as to how those controls are implemented and how the audit request they provided address the controls.

After the interview, the result will be documented in the requirements traceability matrix (RTM) as to whether the applicable NIST-800-53 controls pass or fail based on the detailed testing guide/ assessment objectives obtained for each control from NIST-800-53A. The result, from the control test and the Nessus

vulnerability scan result, are then summarized into the SAR. POA&M is then created for noted findings from failed controls while the ATO is obtained for another 3 years signed by the designated authorizing officer.

I assist the system owners to put this C&A package of SAR (and sometime control waivers/exceptions) and the ATO memo together for the approval of the authorizing officer, for my assigned systems.

- c. **If you are interviewing for Information System Security Officer (ISSO) position**, your daily duties will be: I perform day-to-day support and maintenance of the IT Security program/FISMA compliance for my assigned systems (these could be between 7-10 systems), which include security policies and procedures development and update, audit findings Plan of Action and Milestone (POA&M) management and providing response to audit enquiries and requests. I work with the system owners to maintain the system's required security controls and environment.

**2d. What are some of your achievements or benefits/value added to your clients?**

Name some of these (and **look for opportunity to mention them when you describe what you do as a Security Analyst even when not asked directly for your achievement**):

1. We/I provided subject matter expertise to improve the automated vulnerability assessment of the system servers by recommending update of the Nessus scan policies to turn on additional plugins associated with well know web applications vulnerabilities (silent note: such as CGI Abuse plugins and cross-site scripting (XSS) plugin to detect vulnerabilities that allow attackers to inject codes into the system through the web application).
2. We/I completed the review and development of policies and procedures and developed a complete A&A package in a two month timeframe and received a high performance rating from our client.
3. We/I completed the A&A process ahead of schedule and minimized the systems vulnerability through implementation of security solutions and safeguards tailored to the client's unique environment.
4. We/I assisted in enhancing the client's overall security posture by identifying potential vulnerabilities through vulnerability scanning as well as assessing security controls' operating effectiveness through A&A services and with successful completion of concurrent re-authorization processes for two systems
5. We/I assisted the client to keep current/updated their C&A packages, security policies and procedures, POA&Ms, and assisted with their findings remediation. This helped to improve their overall FISMA failing scorecard to passing scores/grades within six months.

:

**2e. What is the IT security process or steps or How would you explain RMF/C&A/A&A Process to someone else such as a system owner?**

Paraphrase the **6 NIST 800-37 Risk Management steps or FISMA steps/process** in the **Security Assessment and Authorization (A&A) document**, from CATEGORIZE Information System to follow-up MONITOR Security Controls.

Respond as follows, and mention the RMF key words and applicable NIST documents as much as you can to demonstrate deep knowledge of the RMF process:

We perform the A&A process using **NIST 800-37 Risk management Framework** as our guide, and observe the required **6 RMF steps**.

6. As a start, we **CATEGORIZE the information system** being assessed into Low, Moderate or High security impact, using **FIPS 199** as a guide. We use the information types guidance in **NIST 800-60 volume 2** to determine the security categorization of the system based on the required **confidentiality, integrity and availability (CIA)** of the information the system processes or stores. The system overall security categorization is determined by adopting the **“highest water mark”** of information type impact determinations for confidentiality, integrity, and availability.
7. Next, we **SELECT security controls** that are applicable to that system based on its security categorization earlier determined. These security controls, including **primary and applicable control enhancements** are selected from the **18 control families** (silent note: only 17 is applicable to most systems as Program Management (PM) control family is regard as common control and inherited from the head office and therefore only applicable to GSS) in **Appendix D of NIST 800-53** with the relevant detailed **control requirements** and **supplemental guidance** from **Appendix F** of this NIST document. The selected controls are then documented in the security control section of the System Security Plan (SSP).
8. We will then **IMPLEMENT the security controls** selected by addressing how each control is implemented in the **implementation section of the SSP**. This will include the **frequency of performing these controls** as well as the **control type**, such as whether the controls are **system specific, common control, hybrid** (which is a mix of system specific and common control), **inherited** from the environment where the system is hosted or if the control is **not applicable** to that system. We will also indicate the **control status** to show if the controls are currently **in place** or **planned**. We use the **Appendix A of NIST 800-18** as a guide for the developing of SSP.
9. The fourth step we take is to **ASSESS the Security Controls**. Security Assessment Plan (**SAP**) is created to document **assessment schedule, tools and personnel** as well as **obtain approval** of the client for the assessment **approach and scope**, including **Rules of Engagement (ROE)** where vulnerability scanning or penetration testing procedures are included in the assessment. We will conduct the assessment **kickoff meeting** and security controls **interview meeting** with the ISSO and the system owners. We will also create a **Requirement Traceability matrix (RTM) or test cases** to document our assessment of whether the controls **pass or fail using NIST 800-53A** as a guide for determining assessment methods such as when we need to **Examine** policy and procedures, **Interview** personnel with responsibilities for the controls we are testing and whether to perform **Test** by reviewing screenshots of system configuration of such control implementation, especially for the technical controls. The weaknesses noted in our assessment are then reported in the **Security Assessment Report (SAR)** after their **risk level of Low, Moderate or High have been determined** using the risk determination table of **NIST 800-30** during which compensating controls have been considered as well as the **impact and likelihood** of each weakness. The **overall risk level of the system, which could be Low, Moderate or High is then determined** based on the average risk level of the reported weaknesses.

During the assessment, **A&A package items are reviewed** for security/NIST compliance, which include security policy and procedures, System FIPS 199 Categorization, e-Authentication Assessment, Privacy Threshold Analysis (PTA), Privacy Impact Analysis (PIA), Contingency Plan (CP) and Contingency Plan Test (CPT) and POA&M.

5. The next step is to **AUTHORIZE Information System**. This is where the system Authorizing Official signs the system **Authorization to Operate (ATO)** based on the Low or Moderate risk level of the system reported in the **SAR** as well as the existence of the Plan of Action and Milestone (**POA&M**) created to correct audit findings, and the completion of the **A&A Package**. The system is then authorized to operate for another 3 years except major changes occurs that shortens the life-span of that ATO and causes re-authorization.
1. The last step is to **MONITOR Security Controls**. This is **continuous monitoring** (Silent note: this is called ongoing authorization at DHS) where we use **NIST SP 800137** as a guide, and test a **portion (e.g., one-third) of the applicable security controls** annually and perform **periodic (e.g., quarterly) vulnerability scanning**).

## **2f. How do you perform security control testing (SCA) or control assessment?**

Paraphrase the RMF **ASSESSMENT tasks/phase** in the A&A Activities Description section of your A&A handout, starting from SCA Team & Timing, and including the following: FIPS 199 Security Categorization, SCA Kickoff, Assessment Plan (SAP) preparation, Document Request/Audit Request/Evidence Request/PBC List, SCA Interview/Meeting, Perform Vulnerability Scanning/Analysis, down to putting together the SAR, POA&M & ATO (such as the ISSO creating the POA&M from the findings reported in the SAR, and the subsequent signing of ATO by the client's system Authorizing Official).

In the simplest form, to test security controls, you will obtain understanding of how the controls (i.e; controls selected/applicable to that system based on security categorization) are implemented from the SSP (i.e; control implementation statements/section of the SSP) or from interviewing with ISSO and/or system owner. We will then observe the evidence provided to proof/support that the controls are in place, and determine if the control passes or fails. These testing work are documented in the RTM / Test Cases. The failed controls and related findings/weaknesses are then reported in the SAR which is the final report on security assessment (Silent note: this was demonstrated with the homework where RTM was completed).

## **2a. What do you understand by SSP?**

SSP is a plan of action to protect a system from unauthorized access. This document contains the background information and other security details about the system, including its applicable security controls (including NIST 800-53 control requirement and related supplemental guide, control type and implementation status) based on its security categorization and how those controls are implemented on that system. See more details in your A&A Package handout and see example (Control and Non-control sections) in your A&A Package Practice folder

## **2b. What do you understand by POA&M?**

Plan of Action and Milestone (POA&M) is a management tool for tracking corrective action plan and milestones accomplished in addressing and resolving security-related weaknesses/findings. POA&M refers to the plan for correcting an individual weakness. See more details, including example, its content/fields and tracking tools in your POA&M Management handout and Practice folder.

**2i. Do you have any experience with FedRAMP?**

Yes, one of my assigned systems is a FedRAMP system. It is a system hosted by a cloud service provider (Silent note: example are Dropbox, MS Storage). I worked with ATO package completed with FedRAMP templates and the 3PAO that performed the assessment (Silent Note: example: KPMG, PwC). Remember this is same as A&A project except that streamlined/abbreviated A&A templates and key documents are used. Provide one of the 3PAO from your A&A. Also remember that the client will be any of the Cloud Service Providers (CSPs) such as **Dropbox** storage, **AT&T** storage, **Microsoft** cloud, **Verizon** satellite service, and **Amazon** web services, as indicated in the A&A handout.

**2a. Do you have experience working with DOD or DIACAP?**

Not directly with DOD, but some of my systems have interconnection agreements with DOD (example, DLA, NSA), and I reviewed the DIACAP packages for those systems. In addition, I'm very experienced in the RMF C&A process used by federal agencies which is similar to DIACAP, and I understand the DOD has changed to RMF.

(Note that you would have a security clearance if you had a direct experience with DOD beyond DLA which is the civilian agency within DOD).

**2c. How frequently do you interact with your ISSOs or the ISSOs assigned to your systems?**

Daily and as needed based on the demand of my work with them.

**2b. If you are a Security Analyst, do you have experience performing ISSO work?**

Yes, I perform the ISSO's work on some of my assigned systems when the ISSO is not available or my systems whose ISSO have left the organization. In this role, I update security documents, such as policies and procedures, Contingency Plan (CP), Contingency Plan Test (CPT), POA&M and SSP, and I work with the system owners to maintain the system's required security controls and environment (Silent note: You would not have an official ISSO designation letter signed by the CISO since this is a temporary function; and this would also happen where there is no officially assigned Alternate ISSO whom are usually not appointed). (Note that in some security teams/organizations, you may be assigned some systems as an Assessor and different other systems as an ISSO, so that you perform both functions, but not on the same systems, for independence/objectivity purpose, so you are not assessing your own work/same controls that you implemented as ISSO)

**3. What projects have you worked on?**

IT security as part of the Security Assessment and Authorization (A&A), security Controls Assessment (SCA, **also applicable to a commercial company**), vulnerability scanning, vulnerability assessment, POA&M management, IT Security policies and procedures development, update and review, A&A package development and review, response to audit requests and enquiries or audit support/coordination, and PCI DSS compliance audit (**also applicable to a commercial company**). See additional details including more technical projects (like penetration testing and incident response) in the IT Security functions in 2a above.

#### 4. Which clients have you worked on?

- a. Provide federal agencies like Department of Commerce, Department of Labor, Department of Agriculture, Department of Health and Human Services (HHS), and know their branches or operating divisions (including their locations/city which are mostly in Washington DC) where you have worked, such as National Oceanic And Atmospheric Administration (NOAA) for Department of Commerce, US Forest Service for Department of Agriculture, and National Institute of Health (NIH) and Centers for Medicare & Medicaid Services (CMS) for Department of Health and Human Services (HHS) (Note that HHS is located in Rockville MD) (see this link for the full list: <http://www.loc.gov/rr/news/fedgov.html>. Click the agency's name links for their websites and contact tab for their locations). Also know their IT security consulting companies (such as Booz Allen, IBM and Mantech that performed these projects you work on, with whom you worked as an employee or subcontractor. These information are also available on the agencies websites or Google (you can also check this on Google by adding your preferred agency's branch name to Information Assurance, such as "NOAA cyber security contractor"). Check if the firm you are interviewing with is the consultant for the mentioned companies or federal agencies. Also check the PCI DSS handout for the type of companies that comply with PCI DSS if claimed as part of your experience.
- b. If interviewer is interested in commercial project, provide names of companies looked up on Google by industries such as Suntrust or BB&T in banking, Nationwide or Allstates in insurance, and AT&T or Verizon in communication; but be sure to check out their IT security consulting companies, if any, on their websites with whom you have worked as a sub-contractor. Also know their locations where you have worked.
- c. Make sure you have at least one client per company/position or project that is on your resume, as you may be asked which client did you work on when you were with this company, and which client at this other company? If your clients are not well known, you may also Google or check [en.wikipedia.org](http://en.wikipedia.org) for the rough idea of the **asset size**, **revenue** and the **number of employees** of your clients in case you are asked; such as Suntrust bank having asset size of \$172 billion, revenue of \$8 billion and 26k employees as of 2013 financial year. Similar recent relevant numbers for federal agencies such as the Department of Commerce are \$8 billion budget/revenue and 44k employees.
- d. **Is your company the prime or sub-contractor on the project you worked on?** Indicate that your company was a sub-contractor in most cases since the project are usually large and the prime contractors could be known or easily checked on the internet, but know the prime contractor in charge of the project under which you worked as a subcontractor as indicated above.
  - a. Make the timeframe of these projects fall within your IT security experience period.
- a. **What project are you currently working on?**

Provide one of the names of the **projects and clients** mentioned above, such as I'm currently working on Security Assessment and Authorization (A&A) project at the Department of Commerce bank, or POA&M management project at the Department of Agriculture;

or for commercial projects: Security Controls Assessment (SCA) at Suntrust bank, PCI DSS at BB&T bank, or IT Security policies and procedures development at Allstates.

**g. What Systems have you reviewed or supported?**

Provide the names of at least 3 of systems on the first paragraph of your IT Security Introduction document, which include SAP, Oracle Financial, PeopleSoft, Momentum (federal customized Oracle Financial), Identity Management System (IDMS), Physical Access Control Services System (PACS), and GSS or IT infrastructure which consists of operating system, database and network devices, including servers of Mainframe, UNIX, Windows, Oracle database and SQL database.

**h. What do you test or look for, or what are the security tests in IT Infrastructure or router?**

Provide the 5 common tests in your IT Infrastructure handout, such as password settings,

- 1- Password settings being appropriate
- 2- Access to privileged IT functions is limited to appropriate individuals
- 3- Default Accounts and Passwords being changed
- 4- Vendor update/fixes or patches
- 5- Other weak settings/configurations- including disabling unnecessary services.....

Remember that the same test would be performed no matter the example of IT Infrastructure mentioned.

**i. How do you test IT Infrastructure or Windows server or firewall?**

Indicate that you will perform or request vulnerability scanning using a tool like Nessus and select the plugins that are appropriate for testing Windows or firewall, and then analyze the results, in order to correct any identified weaknesses/vulnerabilities.

Remember that it is the plugins and scan preferences defined in the scan policy that is varied in order to test different devices or perform different tests. There are different plugins in Nessus for every device and targeted tests or vulnerabilities, including those relating to software development security tests or vulnerabilities. Refer to the **Nessus Vulnerability Scanning Procedures** in your Practice folder for Other Possible Technical Vulnerability Scanning Questions and Responses.

**j. What type of vulnerabilities do you often come across when you test IT Infrastructure?**

**Missing patches, weak password settings, unnecessary services not disabled, weak configurations** from retention of **temporary privileged accounts** or **system's default account passwords** or allowance of remote code execution which hackers can use to create system backdoors (Silent Note: These are the same as controls tested in IT Infrastructure above)

**k. What type of experience do you have with Linux, Oracle and mainframe security?**

I reviewed security settings on Linux, Oracle and Mainframe servers as part of system security assessment. I also supported systems that run on Linux, Oracle and Mainframe as an IT Security Analyst, as part of the systems assigned to me. In the process, I tested for Missing patches, weak password settings, unnecessary services not disabled, weak configurations from retention of temporary privileged accounts or system's default account passwords. The tests were conducted using vulnerability scanning and selecting plugins applicable to each server.

**I. where are the firewall/IT infrastructure controls classified/reported as part of the NIST control families?**

These are AC and CM based on the 5 common IT Infrastructure tests. SC is also specifically applicable to firewall and other network devices based on its SC-5 Denial of Service Protection and SC-7 Boundary Protection controls.

**5a. What is your disaster recovery plan experience?**

I review and update the Contingency Plan (CP) annually as part of the system security documents, following NIST-800-34 Federal CP Guide (ISSO reviews and updates the CP while IT Security Analyst reviews the update). In the CP update, I ensure the CP remains current with respect to CP resource requirements and recovery priorities based on conducted Business Impact Analysis (BIA) which considers the mission critical nature of the system and its services, as well as backup and recovery methods, and disaster recovery site. I also coordinate (IT Security Analyst, System Owner, and the System Administrator, System developers or maintainers also participate in the CP test, i.e. CPT) the CP test annually for my assigned systems, which includes Tabletop exercise (simulated/scenario discussion type test) and full disaster recovery test at the offsite disaster recovery (DR) location of the company where the systems are recovered from the backup data or tapes. **(CP is the document that contains details of planning for a disaster, while CPT contains the details of the test of that plan).** I prepare CP test result or after-action-report, including any lesson learned from the test (Note that DR location (which could also be alternate processing site in the event of disaster at the primary facility) could be at the company's owned location with servers similar to the ones on site (i.e., **hot site**) to which backup data are replicated/backed up daily remotely or a third-party shared DR facility like Sungard, Verizon Data Center, and Data Foundry). See more details in the Contingency and Contingency Plan task in the A&A package handout.

**5b. How do you implement controls, such as ITGCs, that are currently not in place?**

We will prepare policies and procedures for IT General Controls (ITGCs) such as Access Control procedure (or Standard Operating Procedure (SOP)), and Configuration Management procedure, or update the existing policies and procedures to include these controls. System stakeholders, such as system administrators, system developers, system maintainers and other employees who need to perform these controls will then be informed or trained on the new controls to ensure they understand them. A starting or effective date will then be set to implement or begin to operate with the controls. An audit (Security Control Assessment (SCA)) will then be performed 6 months to 1year after, with walkthrough and detailed testing, to determine if the controls are in place as intended and operating effectively.

**5a. What is change management, change request form, and how to manage change?**

This is the process or controls around making changes to a system. Same as configuration management. It involves requesting change, having the request authorized before development, testing the change in the testing environment, approving the change to be moved to production, and having those tasks performed by different people in or them to archive segregation of duties, to prevent fraud or unauthorized changes

#### **5c2. What is your experience with Configuration management?**

I review configuration management (CM) controls as part of security assessment (if you are an Assessor) or while documenting security control implementation in the SSP or while also preparing or updating the Configuration Management Plan (CMP) (if you are an ISSO). It is the **same as change management**, which is the process of controlling changes made to the system. We typically test or ensure that changes made are **authorized** (by supervisor or designated official) before being made, the **changes are tested** outside the production environment (such as in testing or development environment or server), the changes are **approved** to be moved to production after testing and that there is **separation of duties** (i.e.; SOD) in the change management process, such as ensuring that request for change, development and moving the change to production are done by different people.

(silent note- configuration management is **sometimes** adopted as means to achieving the RMF **continuous monitoring** process as changes are collated by the Configuration Management group on a weekly basis, presented for approval of the change control board (CCB) and the post-change review is then performed to monitor the environment to be sure than no unauthorized changes have been made within the environment, on a continuous/weekly basis).

#### **5d. What do you understand by SDLC-system development lifecycle?**

SDLC relates to development and implementation of new systems. It is the process from **initiation/acquisition to maintenance and the retirement phases** of such systems. Regular change or configuration management controls are tested especially at the maintenance phase of the system, but the **authorization** to acquire (at the initiation phase) new systems (being an IT investment) is provided at the IT steering committee level of the organization which sometime includes the CIO, and sometime the CEO.

SDLC involves the following typical 7 phases:

1. Initiation (system need is identified),
2. Planning and Requirements Definition (end-user information needs are gathered by Business Analysts),
3. Design (desired features and operations are done in demo state),
4. Development and Testing (source codes are written in programming language; and unit, integration, performance and acceptance testing),
5. Implementation (system is installed/deployed to production)
6. Operations and Maintenance (program changes and upgrades are performed),
7. Disposition (system retirement via destruction or after due sanitization from sensitive data).

Note that the simplest and one of the oldest SDLC model/type is the **waterfall model**, which goes through the phases of Initiation, Analysis, Design, Testing, Production/Implementation, and Maintenance one after the other like the motion of a waterfall. **Agile model** which is another popular model is based on iterative and

incremental approach to software development, which focuses on delivering a working software within the shortest possible time, and the SDLC steps are therefore not followed in strict order.

**5e. What tools have you used to track POA&M?**

Provide the tools such as TAF, Xacta, CFACTS, RiskVision or CSAM. Remember to mention that they work the same way, if the one being used by the interviewer is different from the one you are experienced in. Refer to your POA&M Management handout for details.

**5a. What is the content of POA&M?**

Provide details of POA&M elements including estimated dollar value from the POA&M Management document.

**5fb. What are the roles of an**

1/analyst or assessor

2/ issue

3/ system administrator

4/ ciso

5/ system owner

When managing POA&M

**Answer:**

The system administrator and other system stakeholders like Network administrators, database administrators or application developers, typically correct the issues or findings. The ISSO follows up to make sure they are corrected and submits evidence of correction to the POAM tracking tool as proof to close the finding, while the IT Security Analyst reviews the evidence of correction and validates that they have been truly corrected and may approve the closure of the finding within the POAM tracking tool. The system owner has overall responsibility for the system, including findings noted on such system, and the ISSO is merely assisting him to maintain the security of the system with the help of the other stakeholders mentioned here.

CISO has overall responsibility for security of all the systems in the organization, and typically reports to the CIO. The ISSO's working under different system owners in the organization have dotted or indirect reporting line to the CISO when it comes to security.

**5fc. What is IV&V with respect to POA&M?**

Independent verification and validation. This is a check by someone other than the ISSO (i.e., independent person), if security weaknesses or POA&M items they indicated have been corrected have truly been corrected by verifying the evidences they have to support the closure of such POA&M items and validating or confirming that they address the closure of the weaknesses.

**5b. What tools do you use for vulnerability scanning?**

Nessus made by Tenable Inc. feel free to mention one other one from the Vulnerability scanning document since they work the same way, but emphasize that you have mostly used Nessus.

**5h. How did you configure the scan profile, what types of plugins and what access rights do you use for vulnerability scanning?**

Discuss the use of safe Checks in the General profile, credentials, plugins and preferences selected based on the Vulnerability practice materials. Mention that Administrator login and password which are privileged access are used, in order to obtain accurate scan result.

**5c. Under which of the NIST 800-53 controls is vulnerability scanning result reported during the A&A process?**

RA-5: Vulnerability Scanning. This is the control that requires vulnerability scanning to be performed as part of security control assessment.

**How do you match vulnerabilities with their corresponding controls from vulnerability scan result?**

The findings would all be matched with RA-5 which is the control for vulnerability scan requirement. You can not individually match them to separate controls. However, If they are from manual test, they should come matched to the controls tested that failed, and those can be matched to their individual controls.

**5d. What is the difference between waiver and exception?**

A waiver is a temporary risk acceptance to operate the system with current weakness typically for the next 6 months while exception is a permanent risk acceptance not to correct the weakness due to reason beyond the system owner's control or due to the cost of correcting the weakness being greater than its benefit. Both documents are typically signed by the Authorizing Officer that signs the system's ATO. Refer to the A&A document for details.

**5e. How many security control families are in the NIST 800-53 document? 18 control families**

**5f. Which of the NIST 800-53 control families are inherited or common controls?**

These are dash-1 controls, Environmental Protection (PE), Media Protection (MP), Maintenance (MA) and Program Management (MP) controls. Inherited or common controls are the controls present in the data center that systems are hosted which those systems can enjoy without the ISSO having to put the controls in place for their separate systems. This is true of PE, MP and MA, while PM is typically in place at the enterprise/entity level of the organization, such as project or contract management controls, and the systems do not individually need to have them in place.

**5a. What do you understand by technical, operational and management control classes and how many of each do you have?**

Recall TOM 495 formula and details in the A&A document.

**5g. What do you do for system continuous monitoring?**

Continuous monitoring is typically performed by testing a portion (e.g., one-third) of the controls annually (since the whole controls are required to be tested over 3 years period which is the life span of the ATO) and performing periodic (e.g., quarterly) vulnerability scanning of the systems.

**5b. Which NIST 800-53 controls address the need and content of policy and procedures?**

These are the dash-1 controls, such as AC-1, CM-1, and AT-1. Refer to Policy and Procedure handout for details.

**5p. What is a NIST control family such as Audit and Accountability (AU) about, and what would you be looking for to be in place?**

Paraphrase the control based on its name and any of the controls known in that control family such as AU-2 (Auditable Events), respond to this one by saying that it relates to controls in place for logging of auditable events that occur on the system, including defining the nature of such log/events and its review to capture suspicious system activities. AU is very common question, but the question could come from any of the 18 control families; but it will generally not ask for detailed controls within the family but stay at the family name level such as AU rather than AU-2.

**5p2. What type of questions would you be concerned with about AU controls or what type of questions would you ask during security assessment meeting on implementation of AU controls?**

Questions about audit events or logs captured, and how the events of interest are determined and approved before they are set up for capturing, and whether the captured events are reviewed periodically, whether manually or with SIEM tools like ArcSight or Splunk. Specifically, I would draw my questions from the key words of the control requirements in NIST 800-53 Appendix F, especially from AU-2 (**Silent Note:** I would ask questions on each control in the AU family and not just AU-2, especially those control whose SSP implementation statement are not clear to me. Second control in each family generally such as AU-2 gives you the main point or theme of that family).

**5a. What are the penetration test phases/steps, and what are the tools used for the test?**

Paraphrase the 5 steps from Information gathering to Covering Tracks in the Penetration test document. Mention at least 3 of the 8 mentioned tools and their purposes/use, such as password cracker, network or web application exploitation or network protocol analysis/sniffing.

**5b. As a SOC Analyst, what IDS/IPS did you work with and what SIEM tool did you use to collect and analyze security events/incidents?**

IDS/IPS will be Snort made by SourceFire, and the SIEM tool will be the most popular SIEM which is ArcSight made by HP. Remember that are used to collect large volume events from different security logs (including IDS), analyze them and alert the SOC Analysts or even create security incident ticket when escalation is required.

**5c. When are you taking your CISSP test, what does this mean, which organization offers it, and what other relevant certifications do you plan to have?**

Next 1 or 2 months (whichever you are more comfortable with). CISSP is (Certified Information Systems Security Professional) certification offered by (ISC)<sup>2</sup> (International Information Systems Security Certification Consortium).

**5a. Why/How did you change your career to IT Security?**

Response to question of “Why” will be about passion and increasing use of IT.

**Response to “How” may be opportunity at your place of work** and they are ready to train, due to need for IT security professionals. Decide on your story ahead of the interview. There is no wrong or right answer as long as they make sense.

**5u. Why do you think you would be able to cope with IT Security role based on your non-IT background/degree?**

I had college minor in computer science which prepared me for this IT Security career (Note that this minor does not need to be on your resume)

**5a. Could you take a lead or Senior role, or do you have leadership experience?**

Say yes, and say you currently lead 3-5 people on your current security assessment project, and you assign them controls to test, review their work, provide them review comments/feedback and lead the client meetings. You can also indicate that you perform lead roles in all the phases of security assessment which include planning, fieldwork and planning, such as leading the kick-off meeting, walkthrough meetings (or SCA interview) and coordinating the exit meetings, by presenting the draft security assessment report (SAR) to the client, when on Assessment project. Employers often seek candidates for lead roles, in order to be on a safer side. Often the candidates are not required to lead anyone after they are employed. Remember you can easily lead based on your level of training, and don't worry if turns out that you need initial 2-weeks on-the-job assistance. Prepare a story of how you have performed lead role in your current position.

**Silent Note on what to look for when review junior team member's work (also applicable to reviewing ISSO's work, if you are a Security Analyst):**

Look for what they missed that you need to provide them review comments to correct or improve their documentation on, so that the security documentation or deliverables to client are of very good quality. It could be they missed testing or selecting some required controls based on system security categorization. It could be that they did not provide sufficient details in their documentation of how the controls are implemented. It could be inconsistent text fonts in the same paragraph (such as different font types like Times New Romans and Ariel and font sizes 10 and 12), grammatical errors or statements that need to be rephrased for them to make sense. Your ultimate goal is to make them do what you would have done as an experienced person that will minimize or eliminate your own supervisor/manager's review comments, and enable another experienced security analyst to understand what was done from reading the documentation and not have questions.

You must however focus on substance and avoid giving trivial comments that do not add value to the security documentation, just for the sake of having comments. You don't have to have comments if the junior person had done a good job, especially on an old assessment or security documentation where the documentation have been improved with review comments from year to year and you are not aware of any change in the security control environment/process/controls that was not captured; just acknowledge their good job and move on to the next control for review. Make sure the junior person follows all the related organization's quality standards that you are aware of from different orientation and other trainings. If you find a huge omission in quality on system with prior year documentation, discuss them with your supervisor first before passing corrective instructions to junior person as that may have been considered in prior year and may have been deliberately excluded from the documentation or assessment scope and documented in the planning document or memo.

**5w. What is the size of your team and how many security controls were you assigned?**

The size of the team is 12-15. Note that most assessment teams are 3, including the project manager. You would probably share the 18 control families into 3 and each having 6 or more, to leave fewer for the project manager who would also review the team's work. You could also have up to 4 teams in the Security group, making all of you about 12-15. This will include a senior manager (sometime called director) and Partner (sometime called managing director) who will come from the head office to the client site to supervise and review the team's work from time to time, if your employer is a consulting company or firm. Apart from the assessment team, there may be security analyst or compliance team who reviews ISSO's work, and ISSO team of additional 5 members each, taking the entire team size to about 25.

**5a. How many security assessments or other projects have you completed?**

Knowing that a project takes about 3 months, you could only complete 4 a year. Multiply this 4 with the number of years of experience. You would therefore have completed a total of 12 projects (4 projects times 3 years) if you have 3 years of experience.

**5b. Which of the security artifacts are you most comfortable with?**

Give one of the A&A Package documents, such as SSP, POAM. Be sure to know what these documents are and what they contain, in case you are asked to provide that information.

**5c. Which of the NIST security control families are you most comfortable with in testing?**

Provide at least 2 of the 18 control families, such as AT, RA, PL, PS or CA (Silent Note: these are the small and easy control families of 4-6 controls). The reason why you are most comfortable could be because they are the ones you were frequently assigned while on an security control assessment task of A&A project. Mention that you are also familiar with the rest of the control families. If asked for the ones you are least familiar with, you can give the technical ones such as AU and SC, and the reason is because they were not often assigned to you.

**5Aa. Which of the NIST security control families are you least comfortable with in testing?**

Provide at least 2 of the 18 control families like AC and SC or AU (Silent Note: AC and SC are the longest and most technical control families; AC has 25 controls while SC has 44 controls). The reason why you are least comfortable with them would be because they are not often assigned to you for testing on your A&A projects. Mention that you have tested them on very few occasions and open to testing them if situation demands it.

**5Ab. Provide an example of audit finding or security weaknesses you have had on your project before or that you commonly see?**

You can discuss one of the findings in the POAM document contained within your A&A Package folder, such as annual role-based security training not being performed by personnel who have security responsibilities for the tested system (This is an AT-3 control finding and POA&M item 2 rated as of Low risk which relate to System Administrators or ISSOs who should take annual training relevant to the roles as different from the annual basic security awareness training taken by everyone). Another common finding could also be lack of process for the periodic test of backup storage media or tape for system recovery where annual Tabletop contingency plan test is in performed which does not provide opportunity for an annual full disaster recovery that involves recovering from backup media (This is a CP-10 control finding and POA&M item 5 rated as of Medium risk). It could also lack of periodic review of the data center physical access list for continued appropriateness (This is a PE-2 control finding and POA&M item 8 rated as of Low risk)

**5Ac. What do you know by vulnerabilities?** - weaknesses in software that enable an attacker to compromise the integrity, availability, or confidentiality of that software or the data it processes.

**5Ad. What is vulnerability management?** - identifying, classifying, remediating, and mitigating vulnerabilities. The first 3 tasks are done using vulnerability scanner, while mitigation/correction involves tasks like installation of identified missing patches or reconfiguring the network devices such as firewall.

**5Ae. Which vulnerability scanner/scanning tool have you used, and for how long have you used them-** Nessus and WebInspect, for 5 years (depending on the number of your IT Security years of experience).

**5Af. What type of vulnerabilities do you often come across?** – Missing patches, weak password settings, unnecessary services not disabled, weak configurations from retention of temporary privileged accounts or system's default account passwords or allowance of remote code execution which hackers can use to create system backdoors (Silent Note: These are the same as controls tested in IT Infrastructure above)

**5Ag. Have you scanned SQL database before, what type of plugins do you use, and what's the SQL admin ID** - Yes, CGI Abuses and CGI XXS are used to detect cross-site scripting and SQL injection vulnerabilities; the SQL admin account used for scanning is the default DBA account named sa, meaning System Administrator, or regular system administrator accounts assigned to individual DBA's and added to or made members of the sysadmin user group.

**5Ah. How do you manage/track noted vulnerabilities-** We use POA&M, and correct the vulnerabilities based different timeframes such as 30 days for High vulnerabilities, 60 days for Moderate and 90 days for Low ones.

**5Ai. What security compliance benchmarks or checklists do you use for vulnerability scanning?** – Indicate the following benchmarks including their Security Content Automation Protocol (SCAP; pronounced Escarp) discussed in the IT Infrastructure handout: DISA STIGs, United States Government Configuration Baseline (USGCB), Microsoft Security Compliance Manager, CISCO Network Infrastructure Checklist, Vanguard IBM Products Checklist, UNIX Red Hat and Solaris SCAP, and Center for Internet Security (CIS) Benchmark (They are validated by NIST, and available at: <https://web.nvd.nist.gov/view/ncp/repository>), with the following details:

In addition to DISA STIGs, the **National Vulnerability Database (NVD)** provides the **National Checklist Program (NCP)**. The NCP provides detailed low level guidance on setting the security configuration of operating systems and applications. These include manual checklists and the automated/tool-based ones called **Security Content Automation Protocol (SCAP; pronounced Escarp)**. SCAP are typically in human and machine readable **Extensible Markup Language (XML)** format and are run by vulnerability scanners as file attachment. Other popular benchmarks apart from DISA STIG are **United States Government Configuration Baseline (USGCB)**, available at <http://usgcb.nist.gov/index.html>), **Microsoft Security Compliance Manager**, **CISCO Network Infrastructure Checklist**, **Vanguard IBM Products Checklist**, **UNIX Red Hat and Solaris SCAP**, and **Center for Internet Security (CIS) Benchmark**. These checklists and associated SCAP and products are usually used by organizations to establish server configuration settings (CM-6).

**5Aj. What do you use to scan databases?** – Indicate NGS Squirrel and AppDetective, and that you also select plugins in Nessus appropriate for scanning specific databases such as SQL, Oracle or DB2 to achieve the same purpose of using these two database scanners.

**5Ak. In what format do you export the Nessus report for your analysis?** – The report is exported in PDF, but when large number of servers are involved, it is exported in CSV and then saved as Excel for quick analysis and ease of filtering/sorting possible in Excel.

**5AL. What do you understand by server hardening, security control tailoring and OWASP top 10 vulnerabilities?** – Server hardening is the process of applying security control benchmarks or checklists such as DISA STIGs and related SCAP to strengthen the security settings of servers (see details in the IT Infrastructure handout).

Security control tailoring is the selection of security controls that are applicable to the system based on its level of security categorization of either low, moderate or high (see the A&A handout for details)

OWAP top 10 vulnerabilities are the top 10 most critical web application security flaws/vulnerabilities published by OWASP as part of its projects. The most current/2013 OWASP vulnerabilities include (mention 3 or 4 of these) Injection, Broken Authentication and Session Management (XSS), Cross Site Scripting (XSS), Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross Site Request Forgery (CSRF), Using Components with Known Vulnerabilities, and Unvalidated Redirects and Forwards. (see details in the Nessus Vulnerability Scanning Procedures and Tech Q&A in your Vulnerability Scanning practice folder)

**5Am. What are the top IT risks/threats in the current year?** These are:

- (i) Cyber crime- The possibility of being hacked make organizations nervous and it has had damaging effect on companies that were hacked recently, such as Sony Pictures, Target and Office of Personnel Management (OPM);
- (ii) Third parties- Potential risks go beyond the primary organization. It extends to third-parties, such vendors, contractors and professional services suppliers, lawyers and accountants that do business with the primary organization. Organizations are now concerned with weaker security practices by their contractors which could compromise the security at the primary organizations that have network connectivity and share data with them,
- (iii) Bring your own device- As more employees use personal devices, applications and cloud-based storage in the workplace, businesses are in danger of information security risks being exploited by hackers.
- (iv) Absence of adequate security awareness- Organizations need to shift from promoting awareness to creating solutions and embedding security behaviors that reduce risk.
- (v) Privacy and regulation- Several regulations have been created that impose compliance cost and conditions on the safeguard and use of personally identifiable information (PII), with penalties for organizations that fail to sufficiently protect it.
- (vi) Social Media- While a business necessity, social media poses real risks. Organizations need to have appropriate governance in place, to guide responsible use of social media.
- (vii) Cloud Service risks- Cloud solutions can facilitate more rapid, agile, cost-effective and value-driving business transformations, but organizations are concerned with managing service and security risks due to outsourced controls to the cloud service providers, which can be

managed with appropriate service level agreements (SLA) and inclusion of audit right in the cloud service contracts.

**5An. Who are system stakeholders?** These are people such as system owners, system administrators, system developers, system maintainers (usually the company that hosts the system if not in-house) and other employees who support the ongoing maintenance/existence of the system.

**5Ao. What do you understand by risk assessment?** This the process of identifying the risks to system security and determining the likelihood/probability of their occurrence, the resulting impact, and additional safeguards/controls to mitigate/eliminate or reduce the impact (Risk level is a product of likelihood and impact) RA involves determining the threat-sources, threat event/action and vulnerabilities/weaknesses that could be exploited by the threats. The process consists of four steps: (i) *prepare* for the assessment; (ii) *conduct* the assessment; (iii) *communicate* assessment results; and (iv) *maintain* the assessment. (Refer to your handout or NIST 800-30 Risk Assessment Guide for further details).

**5Ap. What is risk management?** This the process of identifying, assessing and reducing risk. This processes includes the following steps: (i) framing risk; (ii) assessing risk; (iii) responding to risk; and (iv) monitoring risk. (Also refer to your handout or to NIST 800-30 Risk Assessment Guide for further details this for further details)

**5Aq. What are the differences between NIST 800-53 revision 3 and rev 4? Or How are your clients dealing with the new revision of the FISMA and NIST 800-53 as compared to the old versions? How long is it taking them to adjust and produce your requests.**

ANS: They are adjusting to the additional control requirements, especially in the configuration management control family such as implementing software usage restrictions (CM-10) and User-Installed Software (CM-11) requirements; and also in the Media Protection control family that added media use restriction (MP-7) (which requires encryption of portable media like flash drives) See the NIST Publication folders for the document named “**NIST sp800\_53\_from-r3-to-r4\_appendix-d2-table\_markup (update)**” that shows the changes in the two revisions in track-changes mode.

**5Ar. What are your experiences in the following areas?:**

- Review log and system data for security issues, malicious threats, and regulatory compliance. Collect, organize and catalog audit evidence. **I have experience using Snort IDS to detect security threats, worms, suspicious network traffic, and then escalated security incidents that require being followed up on till resolution..**
- Prepare internal risk and compliance assessments. Validate IT key controls. Make control, procedural and architectural recommendations to management. **I have tested security controls as part of security assessment, using NIST 800-53 and ISO 27001 and Sans-20 security standards.**
- Analyze and respond to security threats. Conduct patch compliance reviews, penetration tests, vulnerability assessments, and static code tests. **I perform**

monthly or quarterly vulnerability scanning, analyze the result, advise on missing patches that need to be applied and follow up with the Network Operations Center team till the patches are applied. I have also worked as part of this team where I was part of the team that tested the patches and then pushed them to production servers using tools like Tivoli. I have also done some light penetration tests before using Kali Linux and other tools like Metasploit and Wireshark.

- Conduct Disaster Recovery and Business Continuity Planning exercises and reviews. I have worked as Information System Security Officer where I was responsible for the disaster recovery plan documentation and testing of my assigned systems. Exercises conducted included tabletop and functional tests which were done on an annual basis.
- Support the audit cycles for PCI, SOC1, SSAE16, and on-site customer security audits. I have worked on PCI compliance projects where I tested all the PCI data security standards. I have also had to use SOC 1 type 2 reports on service organizations that impacted my assigned systems. These reports were obtained from data centers where some of my cloud-based systems were hosted, in order to assess the adequacy of the controls over financial reporting. I have also used SOC 2 report from data centers like Verizon data center in VA, to report on their IT security controls in order to assess the confidentiality, integrity and availability of their systems and the network in order to see if they would be able to meet our service level agreements (SLA) before signing up with them to hosts our systems remotely for us.

**5As. How do you correct false positives?**

The false positives are corrected by making changes to the configuration settings responsible for reporting the false security weaknesses. The correction could be made by the personnel that is responsible for the reporting device, such as Network/Firewall admin or a SOC Analyst if the errors are occurring from IDS/IPS or vulnerability scanner. The settings may be too restrictive and need to be relaxed or the opposite.

**5At. In what part of the C&A/A&A process is penetration testing often performed? Is it something that is done during the “Assess” phase or “Continuous monitoring”? Or does it differ between different agencies/contracts?**

Pentest is performed during the Assess phase of A&A when required in case of assessing Network or web application.

**5Au. Who is directly responsible for correcting a valid vulnerabilities found in a Nessus scan or IT log Audits, I realize the IT Analyst is responsible for finding and documenting audit findings, but who is actually responsible for correcting them?**

Operating system administrators, Network administrators, or database administrators whose assigned servers are impacted or reported as vulnerable by the vulnerability scan report is responsible for making necessary changes to correct the deficiencies identified in the scan.

Correction may also be made by other stakeholders, such as application developers, depending on the nature of reported vulnerabilities.

**5Av. Is Intrusion Detection software used on site? Or out they typically performed on an off-site Security Operations Command?**

IDS sensors are installed on site, on network devices such as firewall, routers and switches, in order to read and report on any abnormal traffic passing through these devices.

**5Ba. After running Vulnerability scan, what do you do with the high volume of information you get? (Something like that)**

The vulnerabilities are categorized into high, medium and low based on their severity. The high ones are corrected first as soon as possible, and the medium ones next, and then the low ones. Correcting them make the affected systems more secure.

**5Bb. Is it the responsibility of the Cyber Security analyst to select their own plugins for Nessus policies or will they be selected by the ISSO, SO or CISO?**

It is the responsibility of the Cyber Security Analyst to select plugins he considered appropriate for his test. He may share it with the ISSO or CISO if they are interested and wanted to see the coverage of the plugins.

**5Bc. What is the process of SIEM?**

SIEM is used to collect event logs from multiple servers and used to correlate or associate them into meaningful information, and determine if an attack has occurred that needs to be reported/notified to the security analyst, usually in form of email alert, security ticket creation or just placing alert information on the SIEM monitor/dashboard, depending on how the SIEM is configured.

**5Bd. While using SIEM such as ArcSight and Splunk, for server security audit log correlation is it typical for the analyst to select the individual logs to be pulled from the servers themselves or is that the job of the ISSO or SO?**

A SOC Analyst has this responsibility and will work with the ISSO who has overall responsibility for Security, to determine the servers that are within the authorization boundary whose audit events need being protected and correlated. Remember that NIST 800-92 has a list of suggested logs to be included in the review, to include firewall, routers, IDS, anti-virus log, remote access, authentication servers, systems events and application servers.

**5Bf. Is IDS/IPS the same? What's the difference and what does each do?**

They are different. IDS detects security events and report on them, while the IPS prevents them from occurring.

**5Bg. How do you explain Cyber security process or procedure to a novice client or someone who has little idea.**

Explain to the Client how you would secure their network or system.

Paraphrase the RMF steps here, with emphasis on the assessment phase, and less emphasis on the categorization and the ATO if the client is commercial client. You may also be silent in the framework used or replace NIST with ISO or Sans-20 if the client/employer is commercial.

Security Assessment report would be written, vulnerabilities reported, the report would be delivered to management, and the security weaknesses tracked till closed and corrections made to secure the affected systems and environment (this would be the creation of SAR, POA&M and obtaining ATO in case of Federal client). This would be followed with periodic test of some selected controls and vulnerability scanning, in form of continuous monitoring.

**5Bh. What challenges do you face when carrying out Vulnerability scanning or penetration tests?**

(a) The challenges include determining the system boundary and all the systems that would be part of the scope of the assessment, especially where there are no adequate documentation of the network or security environment. This would include determining all the application servers, operating systems, databases and network devices that would be assessed without going out of the intended scope of the assessment.

(b) Also, in the case of penetration testing, I have had to follow up with the management or system owners to sign the security assessment plan that I prepared and obtained their approval of the assessment approach, schedule and the rules of engagements, which also indicates the agreed time-of-day/timing of vulnerability scanning and penetration testing that will have minimal impact on the network performance and the organization users and business.

(c) Other challenges, include getting management support to make all the system stakeholders that need to support the assessment available during the assessment period. These folks are system developers, database admins, network admins, system maintainers and other service providers that need to be interviewed and from which security documentation would be needed.

(d) The challenge that occurs especially at the reporting period is explaining the identified security weaknesses in simple non-technical terms for all stakeholders to understand them, and getting them to recognize the implication or what could go wrong if the weaknesses are not corrected, and getting them to understand that the purpose of the assessment is not to catch or report on any individual, but to work together as a team to enhance the security posture of the organization.

I have always worked diligently, earned the respect of the stakeholders and overcome these challenges on all my engagements.

**5Bi. Do you have experience in proposal writing?**

Yes, I have been involved in responding to **Request for Proposal (RFP)** or Request for Quotation (**RFQ**) on several occasions in order to win business/contract from clients. I have participated in writing the **Technical section** of the proposal in which we indicate our planned approach to executing the project or performing the tasks required by the client, based on the requirements in the **Statement of Work (SOW)** contained in the RFP (Silent Note: SOW specifies the elements expected in the winning proposal such as scope of work, acceptance criteria, deliverable schedule, and period of performance of the prospective contract). I have also participated in writing the **Personnel section** of the proposal in which we put together the relevant profiles and the resumes (in consistent format) of the people/resources that will work on the contract/project, as well as writing the **Pricing section**, where we indicate the number of hours it will take to execute the project and multiply the hours by the hourly rates of each labor category such as partner, manager, senior and staff. I have also assisted the Proposal Manager to collate all the proposal sections for the different quality or color reviews, such as **pink team review** (first review of the whole proposal by the proposal team), and red team review (the final review by the proposal team after an update of

the proposal based on the pink team comments), and the gold team review (review by management or partners) before the proposal is signed off by management and submitted to the client for the contract award, before or on the submission deadline.

**6. Other Non-technical attitude questions**

**(always answer with examples):**

**a. What would your supervisor say about you?**

I will be described as hard-working and someone whom could be relied upon to complete tasks assigned to her by my supervisors due to my speed and the seriousness I attach to assigned tasks and deadlines. **(You may replace these with other positive qualities to customize to your personality)**

In fact, my supervisor regularly made comments that ... give at least one example supporting the qualities above.

**b. Experience working in a team:**

I have always worked in teams consisting of manager, clients, Staff and Senior Consultants/Analysts. I/m used to working in teams as well as working independently on my own. Teaming arrangement occurs on almost all my engagements.

**c. How would you describe your abilities as a team player?**

My experience as a team player includes acting together as a team/being on the same page, speaking with the same voice as a team, taking actions that are in the best interest of the whole team rather than that of a single team member, supporting one another and appearing united as one team in front of the client.

**d. Difficult Conflict Situation with team members and how it was resolved:**

Give an example of how you used maturity or patience to prevent a work situation with that may have turned ugly. It may involve discussing with the team member at an appropriate time in a non-confrontational manner, to let them know what they did and the effect on the team, and providing them opportunity to change and revisit the issue after a week or two to check on changes (especially if you are their supervisor), and then escalating the issue to a higher authority/supervisor if the situation does not change.

**e. How would you deal with a difficult client/or what would you do if a client disagrees with your audit findings?**

This involves trying to resolve the issues to some extent within your abilities and if impossible refer the matter to your manager. The most common source of client's disagreement is over audit findings (for someone in ISSO position, it could be disagreement over the best cause of action or estimated completion date when determining the plan of action in closing a POA&M/finding). Resolving this includes your

being patient, acting with positive and professional attitude to avoid confrontation with the client , and above all trying to understand the client's reason for disagreement and your providing detailed explanation to the client with respect to the source of your findings such as showing the client the PBC item/audit evidence from which the findings were derived (e.g. if the finding is from on password setting such as password complexity or length, show the client the password parameters screenshot that was provided showing the finding) at which point the client may understand your position and then be on the same page with you, failing which you should refer the matter to your manager who may then call the client to understand the source of the client's disagreement and able to resolve the matter.

**f. Experience managing multiple projects:**

I worked on multiple projects on several occasions. Give one or two examples using the different projects, and indicate that there could be an SCA and other projects/tasks going on at the same time and you are assigned to both and working with different teams, and that it is a matter of sharing your time among the projects while keeping your eyes on the completion deadline for each project and making sure they are met..

**a. Concern regarding travel and acceptable percentage:**

I'm currently open to travel for as much as the project requires.

**b. Concern regarding background investigation:**

I don't have problem with background investigation....mention it if you had one completed recently which is recorded in any verifiable database.

**c. Concern about rolling off the sleeves to perform detail work:**

I have always performed staff and senior level work on my projects. I do all that is required to complete the project successfully. My projects and other projects often involve documentation of walkthrough and detailed test of controls, which I documented from start to finish, including documenting noted audit findings/issues.

**d. Response to why you are currently unemployed or looking for job?**

Say things like the contract I'm on is ending soon due to project completion, or my position with my current employer is project-based, and my current project is coming to an end, or that I'm currently on the bench, and I'm trying to get another projects to work on.

You may also say you feel it's time to change to a new place and learn new skills and share your experience if you have been at your current position for more than 3 years.

**e. Why do you want to work for our company?**

Say something positive about the company you are interviewing for as the reason why you would like to work for them. These could be one or two positive things you know about them or that you learned from their website, such as their good reputation, their community involvement/service or the positive impact of their products/services on people, nation or on the community (Do some

research on the company or on its website before your interview to be able to answer this question effectively)

**6. What are your most important achievement?**

You may repeat your strengths mentioned above, or provide at least two examples of some work related achievements that you are proud of. You could also use from the examples provided in 2b above with respect to achievements on benefits/value added to your clients.

**3. Tell me about when you had to do something unexpectedly or when the situation you were in changed suddenly, and how did you respond to it?**

Give an example of when you successfully adapted to a changing situation, or when you were able to think very quickly to respond to a situation which indicates you are flexible and a quick thinker (typically known as ability to think on your feet).

**1. Experience at taking ownership of your projects**

Give an example of when you displayed that you were reliable and responsible to ensure the success of a project. It could be because someone left the project you are on abruptly perhaps for another job or due to transfer during which you took ownership of the task to ensure successful completion.

**2. Experience at making important judgment and decision**

Give an example of when you considered the consequences of at least two work related alternatives or options and you were able to make appropriate decision, based on what is the right or fair thing to do in order to resolve a situation among colleagues or in order to complete a task, and it could mean working late in order to meet a deadline or calling a client in order to resolve a conflict or misunderstanding.

**3. Other Questions:**

- **What are your long- term professional goals?** (to be a Senior Official in charge of Security such as the Chief Information Security Officer).
- **What are you looking for or hoping to get form this company?** (to serve as IT Security Analyst/ISSO (or state your expected role which may include Senior) which is a role I'm very comfortable in and currently perform at my current company. I also hope to work with new people and share my experience with others)
- **What do you like most about your current position? Least?** (I like my current position because it has given me the opportunity to learn, acquire various relevant trainings...and things like opportunity to work with different people and team members, good supervisor or company culture, e.t.c)
- **What do you feel you can contribute to this organization?** (check their website or other internal contacts for any problem they may be having and suggest solution)
- **What is your role within your department?** (yes, a Senior Consultant)
- **Do you supervise or manage people? If so, to what extent?** (yes, two junior Security Analysts. I review their work and provide them performance appraisal)

- **How do you handle stress or perform under pressure?** (very well, taking breaks and working long hours if necessary, and keeping positive attitude and keeping my eyes on the positive outcome of the project)
- **Do you have any question for me/the interviewer?** (ask one or two questions about what you genuinely want to know of (which you would not have known with a quick Google search), and it could be about how the position became open, the type of training or professional development or mentoring provided by the company, interviewer's expectations from the successful candidate, expected attributes of successful employees, any reservation about your ability to join the team, the length of the contract being hired for and how long/years left on it, or questions that ask for more information on the result of your internet research about the company with respect to the company's recent achievements or problems faced.). If you are being interviewed as a contractor, avoid questions that are tailored to direct-hire positions and not someone being hired as a contractor, such as those about promotion or training.
- **How do you keep current with IT risks or events?** Indicate that you keep current with subscribing to news feed **from (ISC)2** that offers the CISSP certification, and using other IT Security websites like [infosecnews.org](http://infosecnews.org) and [securityweek.com](http://securityweek.com).

#### **11. Typical Recruiters' and HR Questions-**

**a. What's is your current salary/rate?** (remember to ask for at least \$70 - \$80K per annum and also provide the equivalent hourly rate of \$35- \$38 per hour when divided by annual hours of 2080 and rounded up). **The reduction from \$80K may happen if you are interviewing for a job outside DC area where cost of living is lower and adjusted in their salaries.** Employers will often let you know if they are unable to pay what you ask for and you may then need to be flexible.

**b. Is that W2 or 1099? Which of these two are you open to at this time?** (remember the preference is W2, and this mostly require annual pay, while 1099 is mainly for contracts which mostly require hourly rate and pay higher rate such as \$45 to \$50 per hour for Senior Security Analysts which translate into about \$93K to \$104K per annum when multiplied by 2080 hours). Be sure to know the bi-weekly and monthly gross amount of your current pay, in case asked.

**c. Does current salary include benefits (vacation, holiday 401k) and bonus?** (No, the current salary does not include these, that is my base salary ( Note that base pay is the annual salary divided by 12 months or 24 forth-nights to arrive at your monthly or two-weekly pays) Also note that bonus means performance bonus paid to you as extra when you score typically at least 4 out of 5 in your annual performance appraisal, and it is usually 5- 10% of your base pay, and paid to you in bulk usually a month or two after your fiscal year-end.

**d. Are you currently on full time or contract employment?, and which of these two are you looking for?** (I'm currently on a full-time employment, but I'm open to either full-time or contract employment) Note that the possible reason you would be open to contract

employment while you are on full-time employment is because of higher rate or because you would like to work for yourself.

**e. What are your:**

- **Expected Rate:** (\$5-10K more than the amount you currently earn, and also per hour)
- **Current Location:** MD
- **Work Authorization:** (permanent resident/Green Card or US Citizen)
- **If not a US Citizen or without security clearance, how are you able to work on government projects?** (US Citizenship or security clearance is not required on the government projects that I worked on. These are federal agencies like Department of Commerce, Department of Labor and Department of Health and Human Services (HHS)). All that was required was a basic background investigation involving credit checks and a search through the County records. (Note that only the Department of Defense (DOD) such as Army, Navy, Airforce, Marine Corp projects require security clearance; even a project at the DLA-Defense Logistics Agency which is a civilian arm of the DOD only requires Public Trust Clearance or regular background investigation like all other civilian federal agencies earlier mentioned above)
- **Availability (typically 2 weeks after offer, not immediately which shows you are jobless; but be flexible and be willing to resume earlier if the employer wants you to resume earlier. Ask when they need you to resume and say you would work things out with your current employer, wrap up your work and resume on the date requested.)**
- **Why do you earn up to \$80K as a Consultant?** (because I'm a Senior Consultant. Note that Consultant is the equivalent of entry level Staff or Associate in consulting. Feel free to take Staff role if okay with it but know that salary there is about \$60-65K)

Note- Also remember to **go for W2 instead of form 1099 salary option** as W2 will have you on your employer's payroll and give you the vacation and holiday benefits (vacation, holiday 401k which are extras and not included in the base pay) as well as allow you to claim unemployment insurance if you need to. Form 1099 pays higher rate but without any benefit (and you are not on the payroll and will typically provide monthly invoice to your employer on your hours worked multiplied by your hourly rate), and you may owe tax at year end if you are not careful as your employer will not deduct and pay your tax to government on your behalf. Both W2 and IRS form 1099 are just IRS tax payment options. Provide annual salary as well as hourly rate when asked for your current salary based on the division of your annual salary by 2080 hours as recruiters can't do the conversion for you.

**Other Tips:**

**1a. Interview Preparation Advice/Areas of Concentration (AOC):**

As with all interviews, make sure you read your IT Infrastructure and Network Security Protocols handouts and the pictures in your computer folder. Look up and get familiar with most of the items indicated on the job description as to how you have experienced them, and say **ALL** you know about

each topic when asked. You already know a lot about these topics and that will often impress and exceed the interviewer's expectation, and make them unable to ask further questions as you would have touched their potential further questions.

Most of those are A&A, Risk Assessment and its report RAR, POA&M Management and Vulnerability scanning. Read those and be able to quote as many of the NIST documents as much as possible from the A&A RMF process, especially the Security Assessment step.

Also remember to have the list of your clients, the project you are currently working on, the number of members in your team, your role in the team, and one or two meaningful questions for the interviewers. Also get ready your stories ready to each of the attitude questions.

1b. When interviewing for a commercial client projects:

Make sure you read your IT Infrastructure handouts and the pictures in your computer folder. Also prepare for some experience discussion on IDS such as Snort and SIEM tool such as ArcSight, and how you have reviewed security events log in the past as part of AU control family. Also look up and get familiar with most of the items indicated on the job description as to how you have experienced them, and again say ALL you know about each topic when asked.

After getting the job, and while waiting to resume, spend some time to revise your handouts all over, and practice your hands-on homework. On your first day at work, be prepared to respond to questions like, where or what projects were you working on before, similar to telling them about yourself, in case your colleagues ask in trying to get to know you.

2. For further attitude questions and responses, you may buy the text book titled "Perfect Phrases for the Perfect interview" by Carole Martin.

1. Experience requirement (3-5 years) - 3 years minimum for IT Security; 3 years is good for flexibility to switch between Junior and Senior positions. Position on resume may be IT Security or other titles without Senior for such flexibility.

2. Reference list-Recruiters will often request this which should include your colleagues' and supervisors' Name, relationship with you, email address, phone number, company name where they worked with you. Be sure these are matched to the companies on your resume.

3. Don't waste time with recruiters, except those who show seriousness they have position to fill and Insurance companies who want you to come and work for commission calling you for positions that do not match your background.

4. Do internet research on the employer or the client you are being employed for, and check on any problem faced and suggest solutions, indicating that know you know how to solve the problem. This often turns interviews into discussion asking for your insight on solving the problem and work in your favor.